



# CVE-2017-8038

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2017-8038
<b>State</b>	PUBLIC
<b>Assigner</b>	security_alert@emc.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-11-27 10:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	In Cloud Foundry Foundation Credhub-release version 1.1.0, access control lists (ACLs) enforce whether an authenticated

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Pivotal Software</a>	<a href="#">Credhub-release</a>	1.1.0	All	All	All
Application	<a href="#">Pivotal Software</a>	<a href="#">Credhub-release</a>	1.1.0	All	All	All

## References

Reference	Source	Link	Tags
CVE-2017-8038: Credentials readable from CredHub endpoint   Cloud Foundry	CONFIRM	<a href="http://www.cloudfoundry.org">www.cloudfoundry.org</a>	Issue Tracking, Third
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**